Science & Technology Facilities Council
Rutherford Appleton Laboratory

Adding Secure Services to ESG

Philip Kershaw, BADC

British Atmospheric Data Centre
NATIONAL CENTRE FOR ATMOSPHERIC SCIENCE
NATURAL ENVIRONMENT RESEARCH COUNCIL

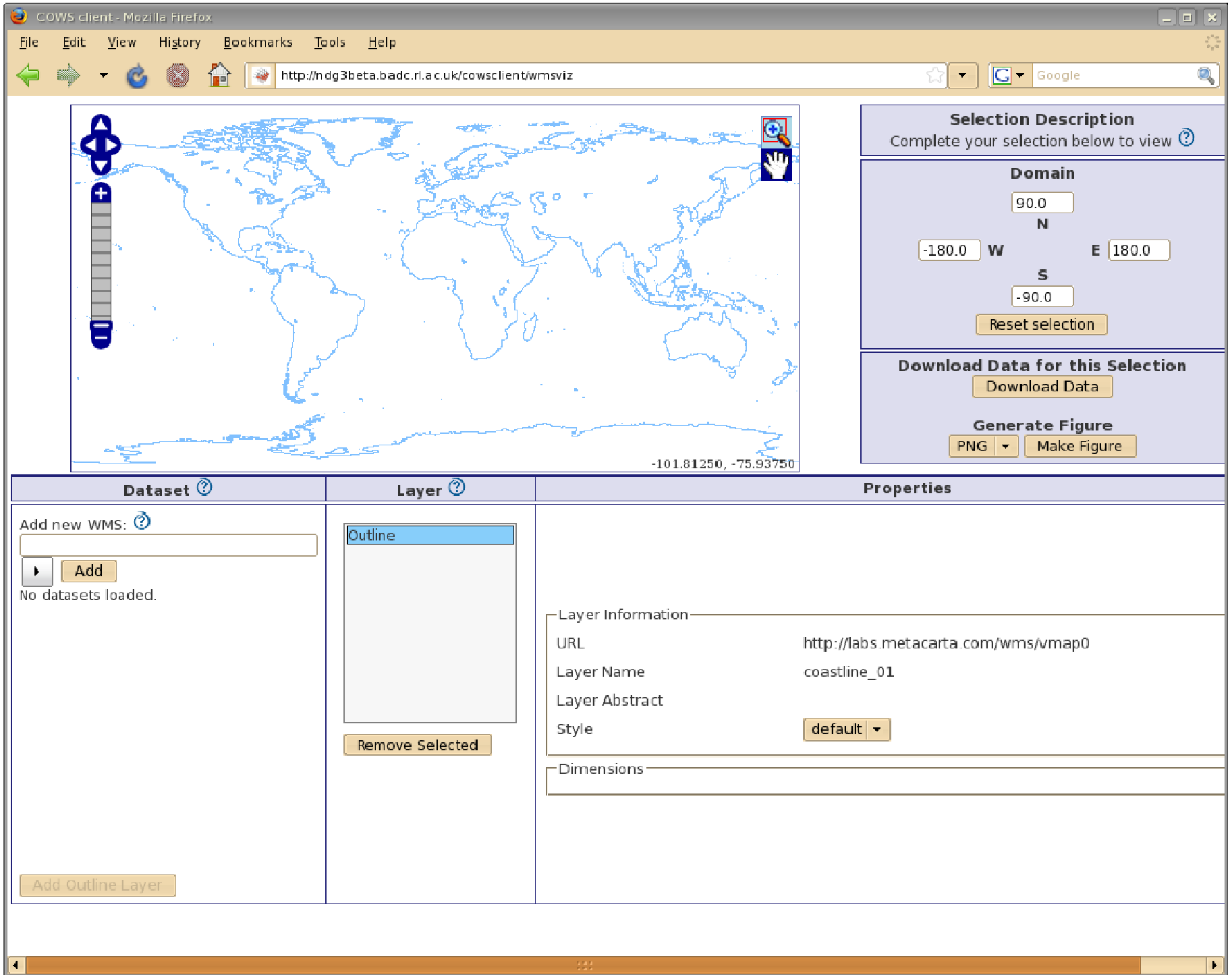
Introduction

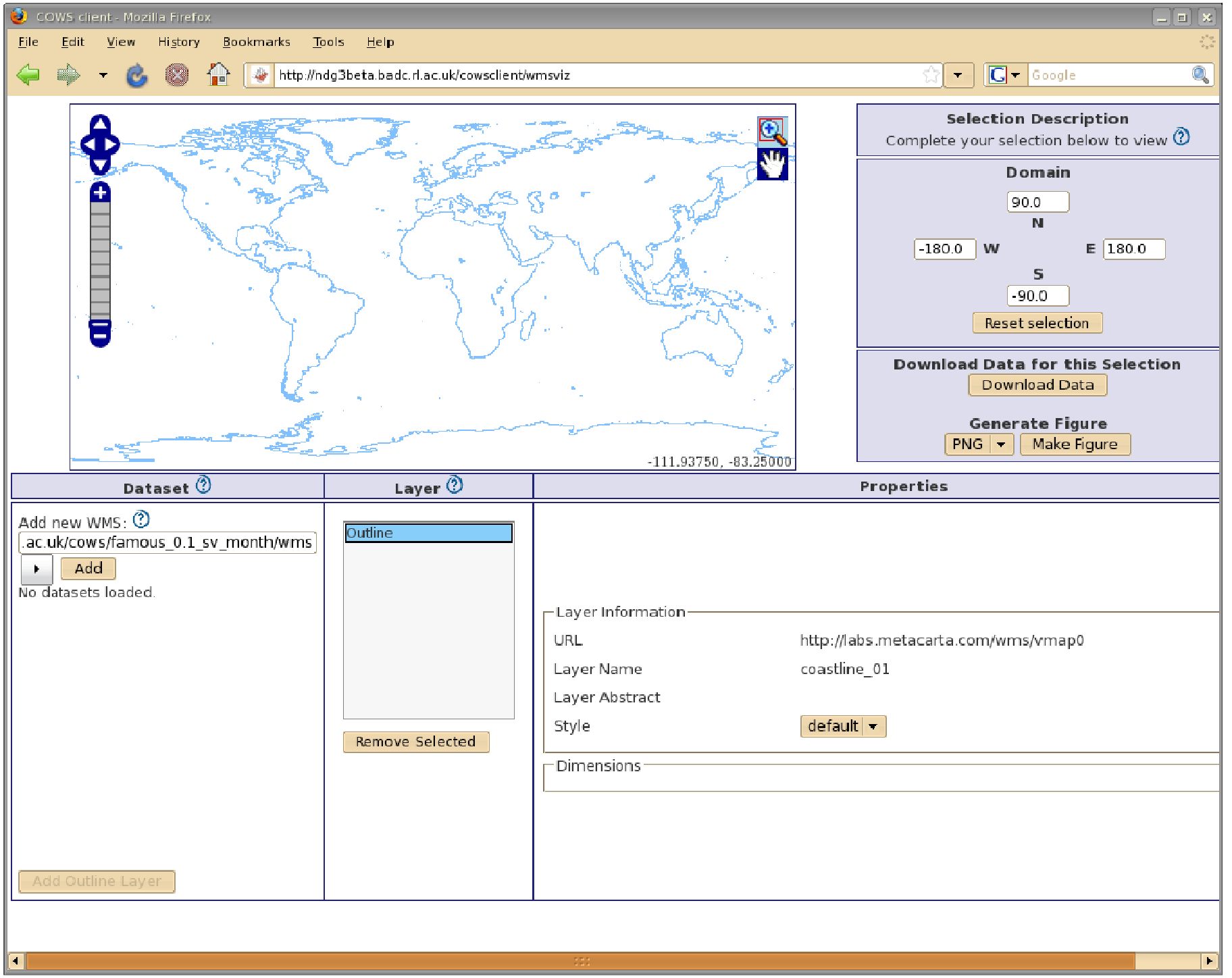
Cows access control in Oxfordshire

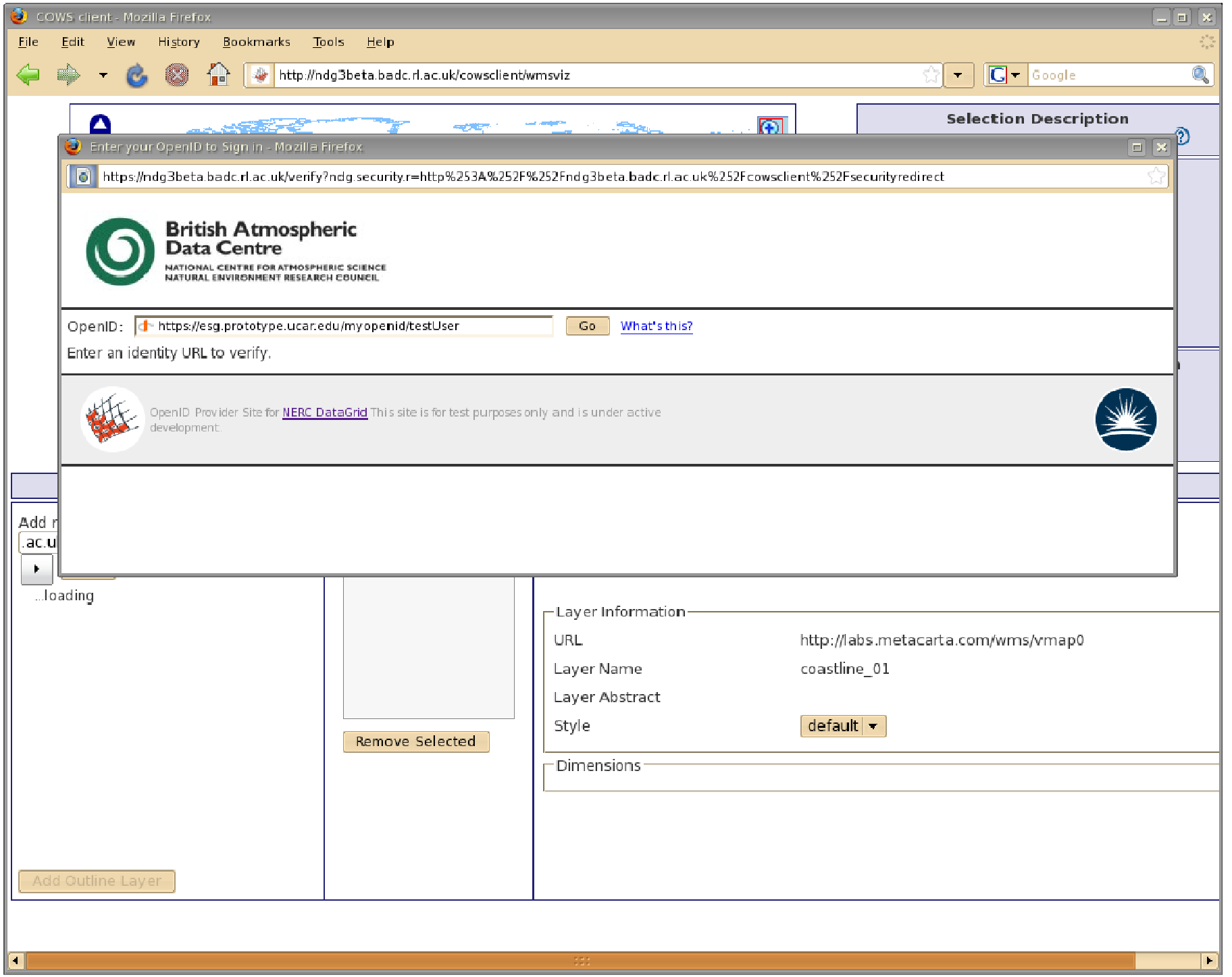
- Overview of access control architecture for ESG
  - What are the interfaces required in order for an institution to link with other organisations in the federation?
- How is this being implemented with data access services at the BADC:
  - Securing PyDAP the Python OPeNDAP implementation
  - And COWS: Our Python based OGC services implementation

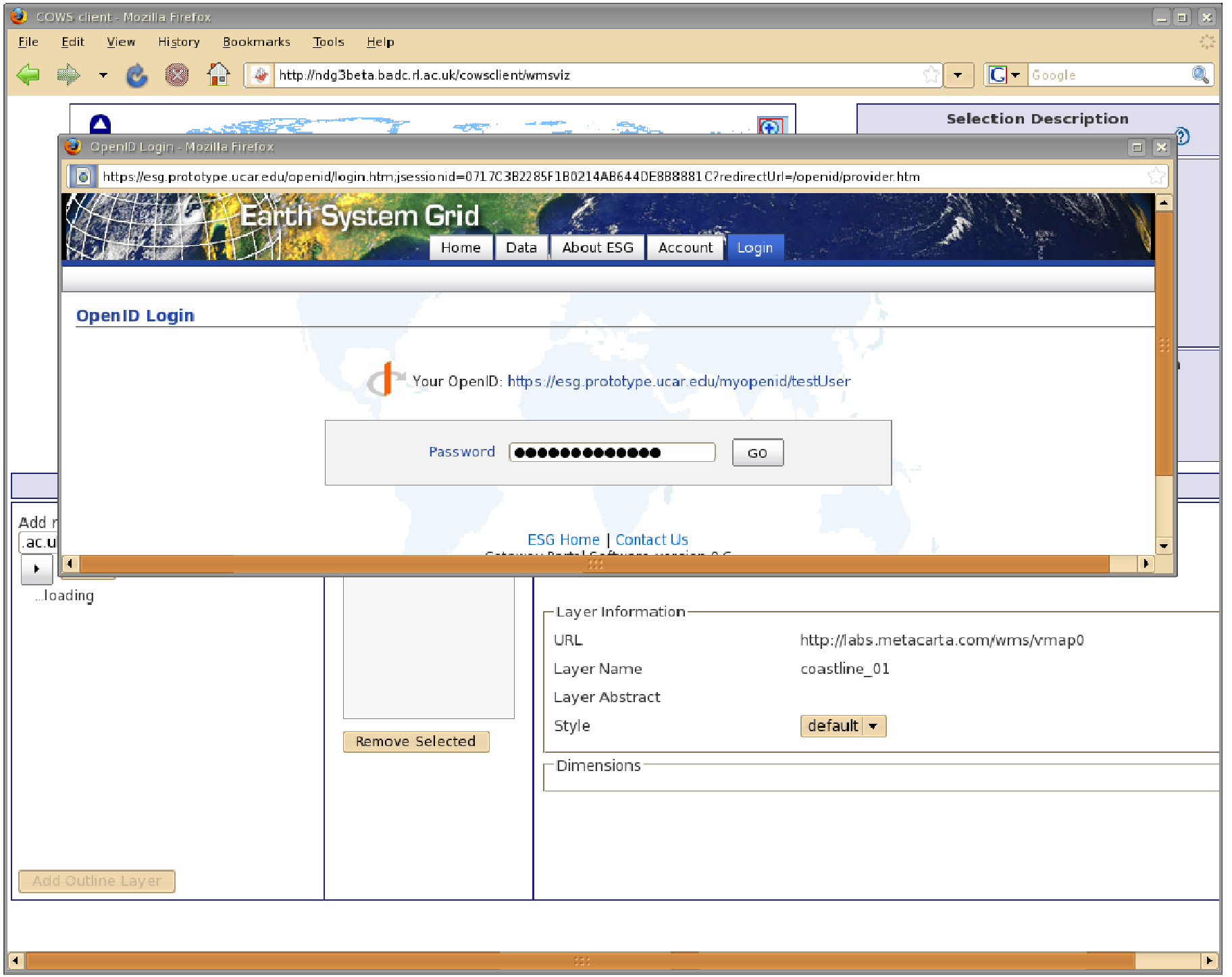
Federation Security 'Glue'

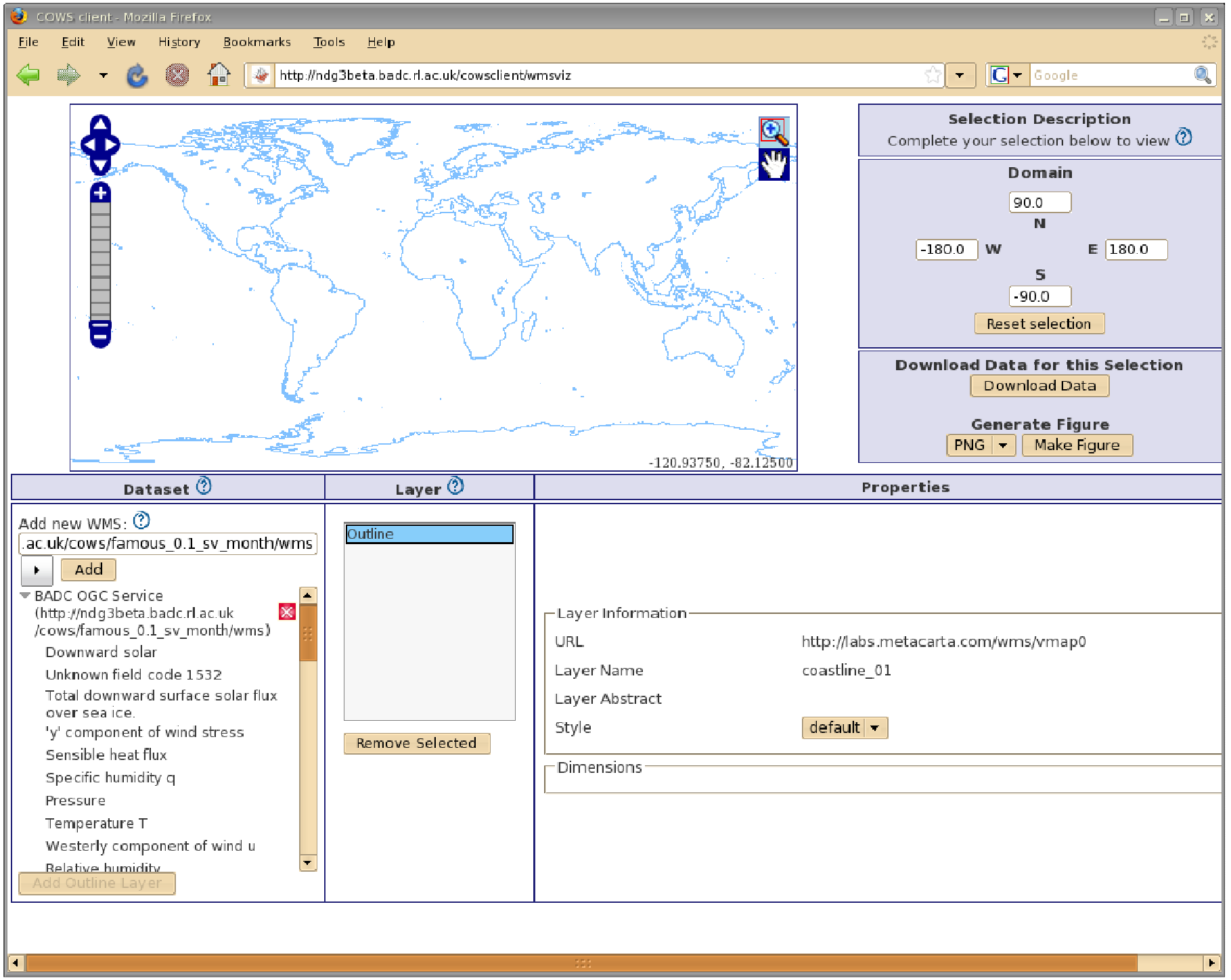
- What are the security interfaces between organisations?
- Security software needs to address:
  - Who are you?
  - … but not enough we also need, to answer: *Where are you from?*
    - **OpenID** – identity URL
    - **MyProxy** – user certificate
    - In both case they identify *you* and your *home institution*
  - What can you do? – user attributes
    - **Registration Service** registers user with given attribute(s)
    - **Attribute Service** enables an authorisation service to query user's attributes
- The interfaces are:
  - OpenID
  - MyProxy
  - Attribute Service
  - Registration Service
- Demonstrating …


COWS client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://ndg3beta.badc.rl.ac.uk/cowsclient/wmsviz
Google
-101.81250, -75.93750
Selection Description
Complete your selection below to view
Domain
90.0
N
-180.0 W
E 180.0
S
-90.0
Reset selection
Download Data for this Selection
Download Data
Generate Figure
PNG
Make Figure
Dataset
Layer
Properties
Add new WMS:
Add
No datasets loaded.
Outline
Remove Selected
Layer Information
URL
http://labs.metacarta.com/wms/vmap0
Layer Name
coastline_01
Layer Abstract
Style
default
Dimensions
Add Outline Layer


COWS client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://ndg3beta.badc.rl.ac.uk/cowsclient/wmsviz
Google
-111.93750, -83.25000
Selection Description
Complete your selection below to view
Domain
90.0
N
-180.0 W
E 180.0
S
-90.0
Reset selection
Download Data for this Selection
Download Data
Generate Figure
PNG
Make Figure
Dataset
Layer
Properties
Add new WMS:
.ac.uk/cows/famous_0.1_sv_month/wms
Add
No datasets loaded.
Outline
Remove Selected
Layer Information
URL
http://labs.metacarta.com/wms/vmap0
Layer Name
coastline_01
Layer Abstract
Style
default
Dimensions
Add Outline Layer


COWS client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://ndg3beta.badc.rl.ac.uk/cowsclient/wmsviz
Google
Selection Description
Enter your OpenID to Sign in - Mozilla Firefox
https://ndg3beta.badc.rl.ac.uk/verify?ndg.security.r=http%253A%252F%252Fndg3beta.badc.rl.ac.uk%252Fcowsclient%252Fsecurityredirect
British Atmospheric Data Centre
NATIONAL CENTRE FOR ATMOSPHERIC SCIENCE
NATURAL ENVIRONMENT RESEARCH COUNCIL
OpenID: https://esg.prototype.ucar.edu/myopenid/testUser
Go
What's this?
Enter an identity URL to verify.
OpenID Provider Site for NERC DataGrid This site is for test purposes only and is under active development.
Add r
.ac.u
...loading
Remove Selected
Add Outline Layer
Layer Information
URL
http://labs.metacarta.com/wms/vmap0
Layer Name
coastline_01
Layer Abstract
Style
default
Dimensions


COWS client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://ndg3beta.badc.rl.ac.uk/cowsclient/wmsviz
Google
Selection Description
OpenID Login - Mozilla Firefox
https://esg.prototype.ucar.edu/openid/login.htm;jsessionid=0717C3B2285F1B0214AB644DE8B8881C?redirectUrl=/openid/provider.htm
Earth System Grid
Home
Data
About ESG
Account
Login
OpenID Login
Your OpenID: https://esg.prototype.ucar.edu/myopenid/testUser
Password
GO
ESG Home | Contact Us
...loading
Remove Selected
Layer Information
URL
http://labs.metacarta.com/wms/vmap0
Layer Name
coastline_01
Layer Abstract
Style
default
Dimensions
Add Outline Layer

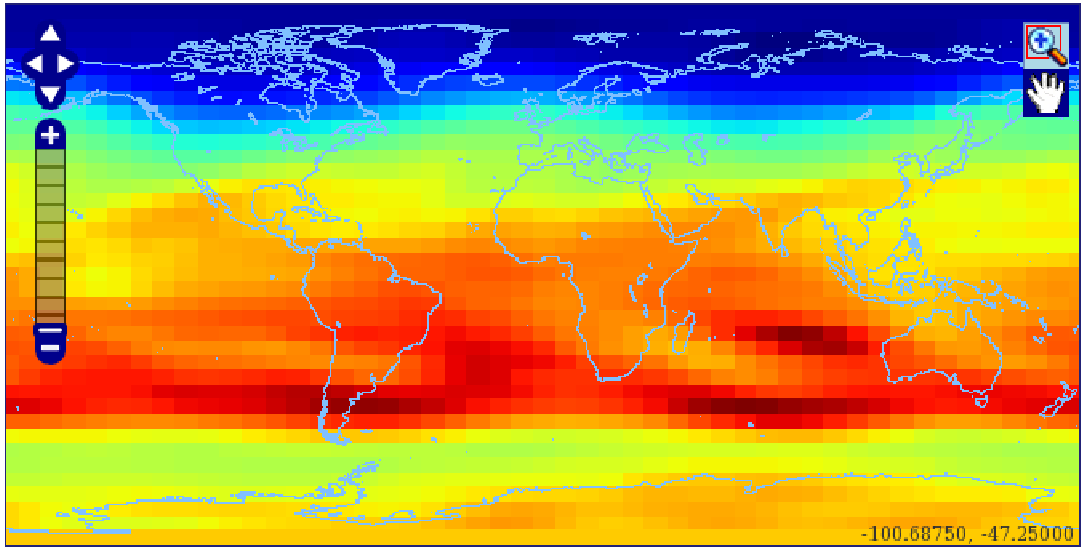

COWS client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://ndg3beta.badc.rl.ac.uk/cowsclient/wmsviz
Google
-120.93750, -82.12500
Selection Description
Complete your selection below to view
Domain
90.0
N
-180.0 W
E 180.0
S
-90.0
Reset selection
Download Data for this Selection
Download Data
Generate Figure
PNG
Make Figure
Dataset
Layer
Properties
Add new WMS:
.ac.uk/cows/famous_0.1_sv_month/wms
Add
BADC OGC Service
(http://ndg3beta.badc.rl.ac.uk
/cows/famous_0.1_sv_month/wms)
Downward solar
Unknown field code 1532
Total downward surface solar flux over sea ice.
'y' component of wind stress
Sensible heat flux
Specific humidity q
Pressure
Temperature T
Westerly component of wind u
Relative humidity
Add Outline Layer
Outline
Remove Selected
Layer Information
URL
http://labs.metacarta.com/wms/vmap0
Layer Name
coastline_01
Layer Abstract
Style
default
Dimensions

COWS client - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://ndg3beta.badc.rl.ac.uk/cowsclient/wmsviz

Google



Selection Description

Complete your selection below to view

Domain

90.0

N

-180.0 W E 180.0

S

-90.0

Reset selection

Download Data for this Selection

Download Data

Generate Figure

PNG Make Figure

Dataset	Layer	Properties

Add new WMS:

.ac.uk/cows/famous_0.1_sv_month/wms

Add

BADC OGC Service (http://ndg3beta.badc.rl.ac.uk/cows/famous_0.1_sv_month/wms)

- Downward solar
- Unknown field code 1532
- Total downward surface solar flux over sea ice.
- 'y' component of wind stress
- Sensible heat flux
- Specific humidity q
- Pressure
- Temperature T
- Westerly component of wind u
- Relative humidity

Add Outline Layer

Outline

#0 air_temperature

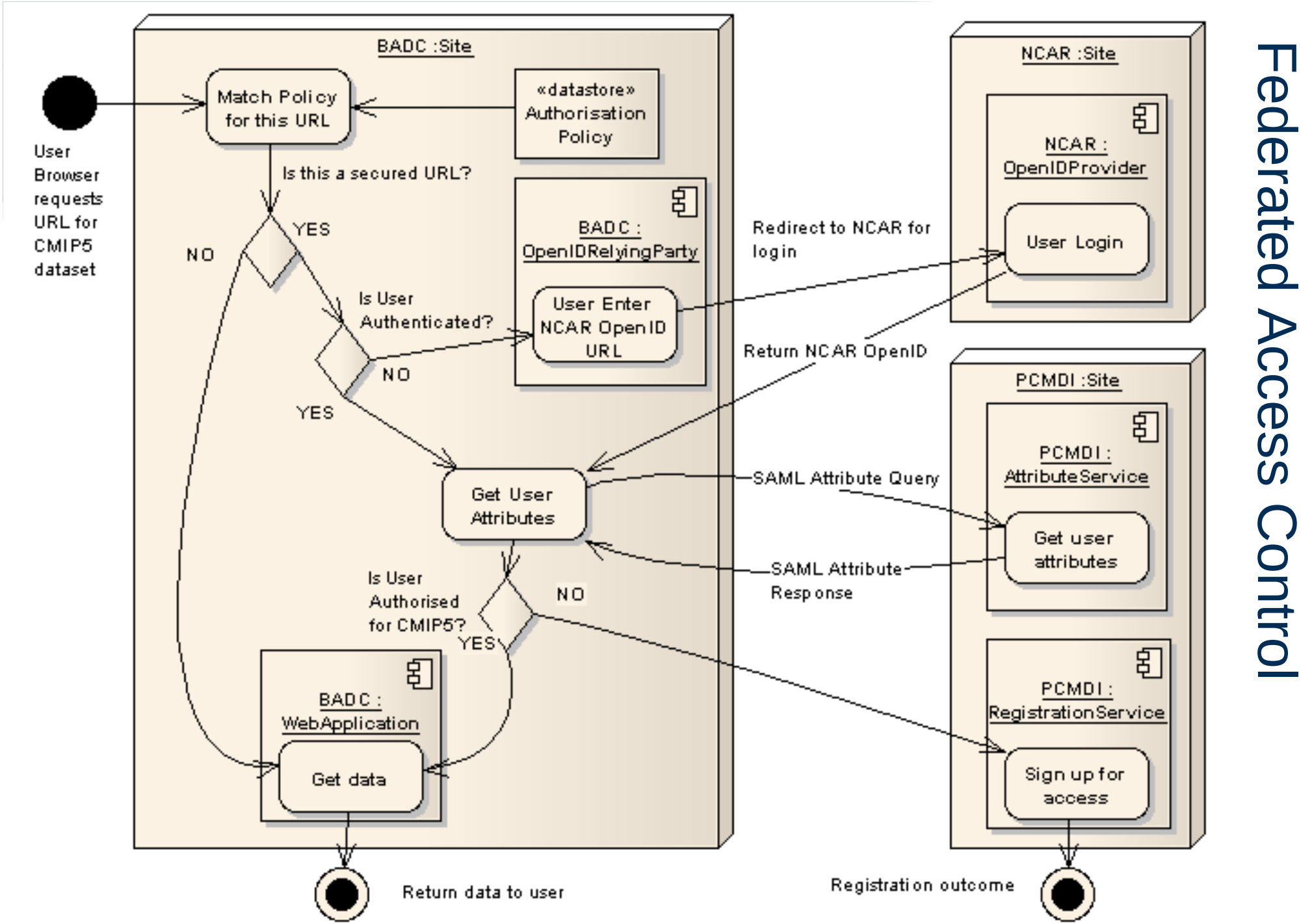
Remove Selected

Layer Information

URL	http://labs.metacarta.com/wms/vmap0
Layer Name	coastline_01
Layer Abstract	
Style	default

Dimensions

Federated Access Control



Python WSGI Middleware

- Building blocks for server side middleware
- Each middleware piece can intercept an incoming client request and operate on it or pass it to the next in a chain
- Server side functionality can be assembled from ‘prefabricated’ units in a flexible manner at deployment in a configuration file:

```
[pipeline:main]
pipeline = AuthenticationFilter
           AuthorisationFilter
           OpenIDRelyingPartyFilter
           PyDAPServerApp
```

Non-Browser Based Access

- OpenID is unsuitable for non-browser based HTTP clients
- These are important for download services and services like OPeNDAP
- Require single sign-on: address *who are you?* but also *where are you from?*
- MyProxy fits e.g.

```
$ python
>>> from myproxy.client import MyProxyClient
>>> myProxy = MyProxyClient(hostname='myproxy.ceda.ac.uk')
>>> certificate, privateKey = myproxy.logon('philipk', <password>)
```

Secure wget OPeNDAP Request

$ wget http://ndg3beta.badc.rl.ac.uk/dap/rapid/chime/.../chime_co2_1pc_daily_0060_197.oc.nc --no-check-certificate --certificate=./user.crt --private-key=./user.key --keep-session-cookies --save-cookies=cookie.txt --cookies=on

- The server security middleware intercepts the request and redirects the client to HTTPS endpoint in for authentication
- wget follows the redirects and the user certificate and key obtained from MyProxy authenticate the request against a SSL endpoint
- The server sends another redirect request back to the original netCDF data URL passing a session cookie
- Subsequent requests can use the session cookie saved to avoid the need to re-authenticate
- With this overall method:
  - no modification to the request URL is needed
  - User attribute gathering and authorisation are abstracted away from the client

Security Hooks for OPeNDAP Clients

- We want to collaborate with the OPeNDAP development community to agree a standard security interface
- incorporate the security hooks to enable access for:
  - C, Java and Fortran APIs
  - Application software like IDL and Matlab
- Ensure other OPeNDAP servers can interoperate

Summary

- ESG Secured services deployed at NERC DataGrid beta site:
  - COWS OGC Client: http://ndg3beta.badc.rl.ac.uk/cowsclient/wmsviz
  - Secured PyDAP OPeNDAP Server: http://ndg3beta.badc.rl.ac.uk/dap
- Secured browser based and wget based access available
- Standards based solution has enabled interoperability across implementations: ESG Java – BADC Python
  - Lowered the barriers for broader participation of organisations in the federation
- Next steps: production OpenID and MyProxy deployments at CEDA/BADC
- Questions?